REMARKS

Careful review and examination of the subject application are noted and appreciated.

SUPPORT FOR THE CLAIM AMENDMENTS

Support for the claim amendments may be found in the specification, for example, on page 10 line 11 - page 12 line 11, page 13 line 14 - page 14 line 4 and FIGS. 1-4 and 7, as originally filed. Thus, no new matter has been added.

CLAIM REJECTIONS UNDER 35 U.S.C. §112

The rejection of claim 15 under 35 U.S.C. §112, second paragraph, is respectfully traversed and should be withdrawn.

Contrary to the assertion in the Office Action, claim 15 does not include essential matter **from within** Request For Comment (RFC) 3031. Claim 15 provides the Internet Engineering Task Force **designation** of the document that defines the MPLS network. No matter from RFC 3031 is actually claimed. As such, the Examiner is respectfully requested to either (i) identify the alleged essential material in RFC 3031 for possible copying into the specification or (ii) withdraw the rejection.

CLAIM REJECTIONS UNDER 35 U.S.C. §102

The rejection of claims 1-4, 7-11, 14, 16 and 17 under 35 U.S.C. §102(e) as being anticipated by Hama, U.S. Publication No. 2004/0202171, has been obviated in part by appropriate amendment, is respectfully traversed in part, and should be withdrawn.

Hama concerns network and edge route (Title).

Claim 1 provides a first port configured to receive a first frame having (i) a source media access control (MAC) address and (ii) a first network layer protocol identification immediately following the source MAC address. In contrast, Hama appears to disclose an IP "protocol" field (alleged similar to the claimed first network layer protocol identification) is separated from a source MAC address by the field M4 (see FIG. 20 of Hama) and several other fields (see FIG. 9.9 of Halsall). Therefore, Hama does not appear to disclose or suggest a first port configured to receive a first frame having (i) a source media access control (MAC) address and (ii) a first network layer protocol identification immediately following the source MAC address as presently claimed.

Furthermore, claim 1 provides a **network layer** protocol identification retained while inserting a first MPLS label into the first frame. In contrast, the IP "protocol" field (shown in FIG. 9.9 of Halsall) is actually a **transport layer** protocol identification per the *Encyclopedia of Networking, Electronic*

Edition, by Tom Sheldon, page 528 (Appendix A). One of ordinary skill in the art would appear to understand a transport layer protocol identification is different than a network layer protocol identification. Therefore, the IP "protocol" of Hama is not a network layer protocol identification as presently claimed.

Assuming, *arguendo*, that the "tag protocol" in FIG. 17A of Hama is similar to the claims network layer protocol identification (for which Applicants' representative does not necessarily agree), FIG. 3 of Hama illustrates how the tag information from a VLAN packet is removed (swapped with a VPN label) in forming an MPLS packet. Therefore, Hama does not appear to disclose or suggest a network layer protocol identification retained while inserting a first MPLS label into the first frame as presently claimed. Claims 8 and 17 provide language similar to claim 1. As such, the claimed invention is fully patentable over the cited reference and the rejection should be withdrawn.

Claim 2 provides a circuit configured to receive a second frame having a second network layer protocol identification having a difference value than the first network layer protocol identification. In contrast, Hama only appears to discuss an IP-type network layer protocol. Therefore, Haman does not appear to disclose or suggest a circuit configured to receive a second frame having a second network layer protocol identification having a difference value than the first network layer protocol

identification as presently claimed. Claim 9 provides language similar to claim 2. As such, claims 2 and 9 are fully patentable over the cited reference and the rejection should be withdrawn.

Claims 3, 4, 7, 10, 11, 14 and 16 depend from claims 1 and 8, which are now believed to be allowable. As such, the dependent claims are fully patentable over the cited reference and the rejection should be withdrawn.

CLAIM REJECTIONS UNDER 35 U.S.C. §103

The rejection of claims 5, 6, 12 and 13 under 35 U.S.C. §103(a) as being unpatentable over Hama in view of Civanlar et al., U.S. Publication No. 2004/0213221 (hereafter Civanlar), has been obviated in part by appropriate amendment, is respectfully traversed in part, and should be withdrawn.

Hama concerns network and edge route (Title). Civanlar concerns a system and method for soft bandwidth (Title).

Claims 5, 6, 12 and 13 depend from claims 1 and 8, which are now believed to be allowable. As such, the dependent claims are fully patentable over the cited references and the rejection should be withdrawn.

Claims 18-20 depend from claims 1 and 8, which are now believed to be allowable. As such, claims 18-20 are fully patentable over the cited references and should be allowed.

Accordingly, the present application is in condition for allowance. Early and favorable action by the Examiner is respectfully solicited.

The Examiner is respectfully invited to call the Applicant's representative should it be deemed beneficial to further advance prosecution of the application.

If any additional fees are due, please charge our office Account No. 50-0541.

Respectfully submitted,

CHRISTOPHER P. MAIORANA, P.C.

John J. Ignatowski
Registration No. 36,555
24840 Harper Avenue, Suite 100
St. Clair Shores, MI 48080
(586) 498-0670

Dated: January 10, 2006

Docket No.: 0325.00526

Appendix A

Encyclopedia of Networking, Electronic Edition

Tom Sheldon

Osborne McGraw-Hill
Berkeley New York St. Louis San Francisco
Auckland Bogotà Hamburg London Madrid
Mexico City Milan Montreal New Delhi Panama City
Paris São Paulo Singapore Sydney
Tokyo Toronto

Osborne/McGraw-Hill
2600 Tenth Street
Berkeley, California 94710
U.S.A.

For information on translations or book distributors outside the U.S.A., or to arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact Osborne/**McGraw-Hill** at the above address.

Encyclopedia of Networking, Electronic Edition

1234567890 DOC DOC 901987654321098

ISBN 0-07-882333-1 PPBK ISBN 0-07-882350-1 HRDBK

Publisher
Brandon A. Nordin

Editor-in-Chief
Scott Rogers

Acquisitions Editor
Wendy Rinaldi

Project Editor
Emily Rader

Editorial Assistant
Ann Sellers

Technical Editor
Terè Parnell

Copy Editor
Dennis Weaver

Proofreader
Karen Mead

Indexer
Dan Logan

Computer Designer
Jani Beckwith

Illustrators
Sue Albert
Leslee Bassin
Arlette Crosland
Lance Ravella

Cover Design
Regan Honda

Class B address	128.10.50.25	10000000 00001010 00110010 00011001
Class B subnet mask	255.255.0.0	11111111 11111111 00000000 00000000

As mentioned previously, class C addresses restrict the number of hosts per network to 254. To get around this problem, a *subnetting* scheme was devised that basically divides the host portion of the address into two parts and uses some of the bits to identify subnetworks within your own network. However, there is a trade-off in doing this. If you use some of the bits in the host address to identify a subnet, then you reduce the number of bits that are available for host addressing. This is outlined in the following table. For example, if you split your network into two subnets, you can have 126 hosts per subnet. With 16 subnets, only 14 hosts are possible per subnet.

Subnet Mask	Binary Value of Last Byte	Number of Subnetworks Allowed	Number of Hosts per Subnet
255.255.255.128	x.x.x.10000000	2	126
255.255.255.192	x.x.x.11000000	4	62
255.255.255.224	x.x.x.11100000	8	30
255.255.255.240	x.x.x.11110000	16	14

For the technically inclined, note how the last byte in the subnet mask adds binary 1s to the mask in the second column. In the first case, decimal 128 adds binary 1 to the last byte of the mask. This single bit is the subnet address space, but only two values are possible—binary 0 and 1, so only two subnets are allowed. In the second case, decimal 192 adds two binary 1s to the last byte of the mask. With two bits, four subnets are possible—00, 01, 10, 11.

Alert readers might notice that the number of possible hosts is shy by two. This is because the first and last binary values are used for broadcasting and internal use.

IP Datagram

The IP datagram header, pictured in Figure I-15, is the envelope in which data is transmitted. It is sometimes referred to as a packet, in general discussions. The datagram fields are described in the following list. Note that the maximum length of the datagram including header and data cannot exceed 65,535 bytes.

- **Version** The version number of the protocol.
- **IHL (Internet header length)** Length of the header.
- **Type of service** The various levels of speed and/or reliability.
- **Total length** The total length of the datagram.
- **Identification** If a datagram is fragmented, a value that identifies a fragment as belonging to a particular datagram.

- **Flags** DF (Don't Fragment) or MF (More Fragments). An indication of whether or not this is not the last fragment.
- **Fragment offset** Where the datagram fragment belongs in the set of fragments.
- **Time to live** A counter that is decremented with every pass through a router. When 0, the datagram is discarded.
- **Protocol** The transport layer process to receive the datagram.
- **Header checksum** Error correction for the header.
- **Source address** The IP address of the host sending the datagram.
- **Destination address** The IP address of the host to receive the datagram.
- **Options/padding** Optional information and filler to ensure the header is a multiple of 32 bits.
- **Data** The user data (a variable field, not shown in the figure).

IPv6 (Internet Protocol version 6)

IPv4 has served the Internet community well, but it has limited address space and is causing major problems as more and more hosts connect to the Internet. A solution was developed with the creation of CIDR (Classless Interdomain Routing), which

<table>
<tr><td>Bit 0</td><td></td><td></td><td>16</td><td>31</td></tr>
<tr><td>Version</td><td>IHL</td><td>Type of service</td><td colspan="2">Total length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td>Fragment offset</td></tr>
<tr><td colspan="2">Time to live</td><td>Protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">Source address</td></tr>
<tr><td colspan="5">Destination address</td></tr>
<tr><td colspan="5">Options/padding</td></tr>
</table>

Figure I-15. *IP datagram header*

allocated (without e addresses The IE hammere backward are availa The m comparec address t home ent commanc personal (Global P the plane Internet. You oper display a informat such GPS You coul Anot destinati delivery An e: informat new requ Ther Web site details o may be s

RELATE
Concept Framing Mobile I (Transm

INFORM
IETF (In Task Fo Internet